AMENDMENTS TO THE CLAIMS

1. (Currently Amended) A cryptocommunication system including a transmission apparatus and a reception apparatus, wherein:

~~the~~ said transmission apparatus ~~encrypting~~ is operable to encrypt plaintext to generate ciphertext, ~~performing~~ perform a one-way operation on the plaintext to generate a first value, and ~~transmitting~~ transmit the ciphertext and the first value to ~~the~~ said reception apparatus;~~,~~

~~the~~ said reception apparatus ~~receiving~~ is operable to receive the ciphertext and the first value, ~~decrypting~~ decrypt the ciphertext to generate decrypted text, ~~performing~~ perform the one-way operation on the decrypted text to generate a second value, and ~~judging~~ judge that the decrypted text matches the plaintext when the second value and the first value match;~~,~~

said ~~the~~ transmission apparatus ~~comprising:~~ comprises

first generating means for generating first additional information,~~;~~

first operation means for performing an invertible operation on the plaintext and the first additional information to generate connected information,~~;~~

encrypting means for encrypting the connected information according to an encryption algorithm so as to generate the ciphertext,~~;~~ and

transmitting means for transmitting the ciphertext; and~~,~~

said ~~the~~ reception apparatus ~~comprising:~~ comprises

receiving means for receiving the ciphertext transmitted from said transmitting means,~~;~~

second generating means for generating second additional information which is identical to the first additional information generated by said first generating means,~~;~~

decrypting means for decrypting the ciphertext according to a decryption algorithm, which is an inverse-conversion of the encryption algorithm, so as to generate decrypted connected information,~~;~~ and

second operation means for performing an inverse operation of the invertible operation on the decrypted connected information and the second additional information so as to generate the decrypted text.

2. (Currently Amended) The cryptocommunication system of Claim 1, wherein ~~the~~ said second generating means synchronizes with ~~the~~ said first generation means so as to generate the

second additional information which is identical to the first additional information.

3. (Currently Amended) The cryptocommunication system of Claim 1, wherein:

~~wherein the~~ said first generating means transmits the first additional information;~~,~~ and

~~the~~ said second generating means receives the first additional information and sets the received first additional information as the second additional information.

4. (Currently Amended) The cryptocommunication system of Claim 1, wherein:

~~wherein the~~ said first generating means encrypts the first additional information according to the encryption algorithm so as to generate encrypted additional information, and transmits the generated encrypted additional information;~~,~~ and

~~the~~ said second generating means receives the encrypted additional information, ~~and~~ decrypts the received encrypted additional information according to the decryption algorithm, which is an inverse-conversion of the encryption algorithm, so as to generate additional information, and sets the generated additional information as the second additional information.

5. (Currently Amended) The cryptocommunication system of Claim 1, wherein ~~the~~ said first generating means generates a random number, and sets the generated random number as the first additional information.

6. (Currently Amended) The cryptocommunication system of Claim 1, wherein:

~~wherein the invertible~~said first operation means bit-connects the plaintext with the first additional information so as to generate the connected information;~~,~~ and

~~the~~ said second operation means deletes the second additional information from the decrypted connected information so as to generate the decrypted text.

7. (Currently Amended) The cryptocommunication system of Claim 1, wherein:

~~wherein the~~said first operation means performs an exclusive OR operation on the plaintext and the first additional information so as to generate the connected information;~~,~~ and

~~the~~ said second operation means performs an exclusive OR operation on the decrypted connected information and the second additional information so as to generate the decrypted text.

8. (Currently Amended) The cryptocommunication system of Claim 1, wherein:

~~wherein the~~ said first operation means adds the first additional information to the plaintext so as to generate the connected information;~~,~~ and

~~the~~ said second operation means subtracts the second additional information from the decrypted connected information so as to generate the decrypted text.

9. (Currently Amended) The cryptocommunication system of Claim 1, wherein:

~~wherein the~~said first operation means performs modular multiplication on the plaintext and the first additional information so as to generate the connected information;~~,~~ and

~~the~~ said second operation means performs modular multiplication on the decrypted connected information and ~~the~~ modular inversion of the second additional information so as to generate the decrypted text.

10. (Currently Amended) The cryptocommunication system of Claim 1, wherein

wherein ~~the~~ said first operation means replaces the plaintext expressed in at least one bit based on the first additional information so as to generate the connected information~~,~~; and

~~and the~~ said second operation means inverse-replaces the decrypted connected information expressed in the at least one bit based on the second additional information so as to generate the decrypted text.

11. (Currently Amended) The cryptocommunication system of Claim 1, wherein:

~~wherein the~~ said first operation means stores, in advance, a first conversion table corresponding to the first additional information, and converts the plaintext according to the first conversion table so as to generate the connected information;~~,~~ and

~~the~~ said second operation means stores, in advance, a second conversion table corresponding to the second additional information and being identical to the first conversion table corresponding to the first additional information, and converts the decrypted connected information in a reverse direction according to the second conversion table so as to generate the decrypted text.

12. (Currently Amended) The cryptocommunication system of Claim 1, wherein when ~~the~~ said transmission apparatus encrypts~~, in order to generate ciphertext,~~ the plaintext that has been encrypted and transmitted so as to newly generate the ciphertext~~,~~ and transmits the newly generated ciphertext to ~~the~~ said reception apparatus, and said reception apparatus receives the newly generated ciphertext and decrypts the received ciphertext,

~~and the reception apparatus receives the newly generated ciphertext and decrypts the newly generated ciphertext,~~

~~the~~ said first generating means generates third additional information which is different from the first additional information,

~~the~~ said first operation means performs an invertible operation on the plaintext and the third additional information so as to obtain newly generated connected information,

~~the~~ said encrypting means encrypts the newly generated connected information according to an encryption algorithm so as to obtain the newly generated ciphertext,

~~the~~ said transmitting means transmits the newly generated ciphertext,

~~the~~ said receiving means receives the newly generated ciphertext,

~~the~~ said second generating means generates ~~forth~~ fourth additional information which is identical to the third additional information,

~~the~~ said decrypting means decrypts the newly generated ciphertext according to a decryption algorithm, which is an inverse-conversion of the encryption algorithm, so as to obtain newly generated decrypted connected information, and

~~and the~~ said second operation means performs an inverse operation of the invertible operation on the newly generated decrypted connected information and the fourth additional information so as to obtain newly generated decrypted text.

13. (Currently Amended) The cryptocommunication system of Claim 1, wherein:

~~wherein the~~ said transmission apparatus performs the one-way function on the connected information instead of on the plaintext~~, in order~~ so as to generate ~~the~~ a first functional value;~~,~~

~~the~~ said reception apparatus performs the one-way function on the decrypted connected information instead of on the decrypted text~~, in order~~ so as to generate ~~the~~ a second functional value; and~~,~~

~~and the~~ said reception apparatus judges whether the first and the second functional values match.

14. (Currently Amended) The cryptocommunication system of Claim 1, wherein:

~~wherein the~~ said transmission apparatus further performs, on the plaintext, a different invertible operation from the invertible operation~~,~~ so as to generate first connected information;~~,~~

~~the~~ said transmission apparatus performs the one-way function on the first connected information, instead of on the plaintext, so as to generate ~~the~~ a first functional value;~~,~~

~~the~~ said reception apparatus further performs the different invertible operation on the decrypted text so as to generate second connected information;~~,~~

~~the~~ said reception apparatus performs the one-way function on the second connected information, instead of on the decrypted text, so as to generate ~~the~~ a second functional value; and~~,~~

~~and the~~ said reception apparatus judges whether the first and the second functional values match.

15. (Currently Amended) A cryptocommunication method used by a cryptocommunication system including a transmission apparatus and a reception apparatus, wherein:

the transmission apparatus ~~encrypting~~ encrypts plaintext to generate ciphertext, ~~performing~~ performs a one-way operation on the plaintext to generate a first value, and ~~transmitting~~ transmits the ciphertext and the first value to the reception apparatus;~~,~~

the reception apparatus ~~receiving~~ receives the ciphertext and the first value, ~~decrypting~~ decrypts the ciphertext to generate decrypted text, ~~performing~~ performs the one-way operation on the decrypted text to generate a second value, and ~~judging~~ judges that the decrypted text matches the plaintext when the second value and the first value match;~~,~~

~~the~~ said cryptocommunication method ~~including~~ includes a transmission ~~step~~ operation which is executed by the transmission apparatus and a reception ~~step~~ operation which is executed by the reception apparatus;~~,~~

~~the~~ said transmission ~~step comprising:~~operation comprises

~~a first generating substep for~~ generating first additional information,~~;~~

~~a first operation substep for~~ performing an invertible operation on the plaintext and the first additional information to generate connected information,~~;~~

~~an encrypting substep for~~ encrypting the connected information according to an encryption algorithm to generate the ciphertext,~~;~~ and

~~a transmitting substep for~~ transmitting the ciphertext; and~~,~~

~~the~~ said reception ~~step comprising:~~ operation comprises

~~a receiving substep for~~ receiving the ciphertext transmitted in said transmitting of the ciphertext,~~;~~

~~a second generating substep for~~ generating second additional information which is identical to the first additional information generated in said generating of the first additional information,~~;~~

~~a decrypting substep for~~ decrypting the ciphertext according to a decryption algorithm, which is an inverse-conversion of the encryption algorithm, so as to generate decrypted connected information,~~;~~ and

~~a second operation substep for~~ performing an inverse operation of the invertible operation on the decrypted connected information and the second additional information so as to generate the decrypted text.

16. (Currently Amended) A cryptocommunication ~~Cryptocommunication~~ program stored and used by a cryptocommunication system including a transmission apparatus and a reception apparatus, wherein:

the transmission apparatus ~~encrypting~~ encrypts plaintext to generate ciphertext, ~~performing~~ performs a one-way operation on the plaintext to generate a first value, and ~~transmitting~~ transmits the ciphertext and the first value to the reception apparatus;~~,~~

the reception apparatus ~~receiving~~ receives the ciphertext and the first value, ~~decrypting~~ decrypts the ciphertext to generate decrypted text, ~~performing~~ performs the one-way operation on the decrypted text to generate a second value, and ~~judging~~ judges that the decrypted text matches the plaintext when the second value and the first value match;~~,~~

~~the~~ said cryptocommunication program ~~including~~ includes a transmission ~~step~~ operation which is executed by the transmission apparatus and a reception ~~step~~ operation which is executed by the reception apparatus;~~,~~

said ~~the~~ transmission ~~step comprising:~~ operation comprises:

~~a first generating substep for~~ generating first additional information,~~;~~

~~a first operation substep for~~ performing an invertible operation on the plaintext and the first additional information to generate connected information,~~;~~

~~an encrypting substep for~~ encrypting the connected information according to an encryption algorithm to generate the ciphertext,~~;~~ and

~~a transmitting substep for~~ transmitting the ciphertext; and~~,~~

said ~~the~~ reception ~~step comprising:~~ operation comprises

~~a receiving substep for~~ receiving the ciphertext transmitted in said transmitting of the ciphertext;

~~second generating means for~~ generating second additional information which is identical to the first additional information generated in said generating of the first additional information,~~;~~

~~a decrypting substep for~~ decrypting the ciphertext according to a decryption algorithm, which is an inverse-conversion of the encryption algorithm, so as to generate decrypted connected information,~~;~~ and

~~a second operation substep for~~ performing an inverse operation of the invertible operation on the decrypted connected information and the second additional information so as to generate the decrypted text.

17. (Currently Amended) A recording medium which can be read from by using a computer and which stores a cryptocommunication program used by a cryptocommunication system including a transmission apparatus and a reception apparatus, wherein:

the transmission apparatus ~~encrypting~~ encrypts plaintext to generate ciphertext, ~~performing~~ performs a one-way operation on the plaintext to generate a first value, and ~~transmitting~~ transmits the ciphertext and the first value to the reception apparatus;~~,~~

the reception apparatus ~~receiving~~ receives the ciphertext and the first value, ~~decrypting~~ decrypts the ciphertext to generate decrypted text, ~~performing~~ performs the one-way operation on the decrypted text to generate a second value, and ~~judging~~ judges that the decrypted text matches the plaintext when the second value and the first value match;~~,~~

said ~~the~~ cryptocommunication program ~~including~~ includes a transmission ~~step~~ operation which is executed by the transmission apparatus and a reception ~~step~~ operation which is executed by the reception apparatus;~~,~~

said ~~the~~ transmission ~~step comprising:~~operation comprises

~~a first generating substep for~~ generating first additional information,~~;~~

~~a first operation substep for~~ performing an invertible operation on the plaintext and the first additional information to generate connected information,~~;~~

~~an encrypting substep for~~ encrypting the connected information according to an encryption algorithm to generate the ciphertext,~~;~~ and

~~a transmitting substep for~~ transmitting the ciphertext; and~~,~~

said ~~the~~ reception ~~step comprising:~~operation comprises

~~a receiving substep for~~ receiving the ciphertext transmitted in said transmitting of the ciphertext,~~;~~

~~a second generating substep for~~ generating second additional information which is identical to the first additional information generated in said generating of the first additional information,~~;~~

~~a decrypting substep for~~ decrypting the ciphertext according to a decryption algorithm, which is an inverse-conversion of the encryption algorithm, so as to generate decrypted connected information,~~;~~ and

~~a second operation substep for~~ performing an inverse operation of the invertible operation on the decrypted connected information and the second additional information so as to generate the decrypted text.

18. (Currently Amended) A transmission apparatus ~~which encrypts~~operable to encrypt plaintext to generate ciphertext, ~~performs~~ perform a one-way operation on the plaintext to generate a first value, and ~~transmits~~ transmit the ciphertext and the first value, ~~the~~ said transmission apparatus comprising:

first generating means for generating first additional information;

first operation means for performing an invertible operation on the plaintext and the first additional information to generate connected information;

encrypting means for encrypting the connected information according to the encryption algorithm so as to generate ciphertext; and

transmitting means for transmitting the ciphertext.

19. (Currently Amended) A reception apparatus ~~which receives~~operable to receive, from a transmission apparatus, ciphertext and a first value, wherein:

the transmission apparatus encrypts plaintext to generate the ciphertext, performs a one-way operation on the plaintext to generate the first value, and transmits the ciphertext and the first value to said reception apparatus;

said reception apparatus is operable to ~~decrypts~~ the ciphertext to generate decrypted text, ~~performs~~ perform the one-way operation on the decrypted text to generate a second value, and ~~judges~~ judge that the decrypted text corresponds to the plaintext only when the second value and the first value match; and~~,~~

~~the transmission apparatus encrypting the plaintext to generate the ciphertext, performing the one-way operation on the plaintext to generate the first value, and transmitting the ciphertext and the first value,~~

~~the~~ said reception apparatus ~~comprising:~~comprises

receiving means for receiving the ciphertext from ~~the~~ said transmission apparatus of Claim 18;

second generating means for generating second additional information which is identical to the first additional information;

decrypting means for decrypting the ciphertext according to a decryption algorithm, which is an inverse-conversion of the encryption algorithm, to generate decrypted connected information; and

second operation means for performing an inverse operation of the invertible operation on the decrypted connected information and the second additional information so as to generate the decrypted text.